# ECE 435 – Network Engineering
# Lecture 13

Vince Weaver

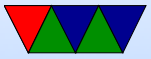
http://web.eece.maine.edu/~vweaver

vincent.weaver@maine.edu

19 October 2016

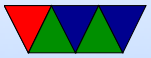
# Announcements

- HW#5 posted, due next Wednesday



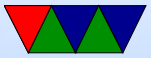
# ARP – address resolution protocol

- Some way to map IP to MAC
- Could have a central server on subnet that could be queried
- Internet uses other way. When need a mapping, broadcast to the subnet, "who has this IP"
- device reply with its IP and MAC (unicast)
- These are cached
- Timeout in case you reassign
- TODO: ARP Packet?



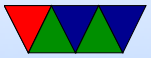
# RARP/BOOTP

- Some cases need to do RARP (Reverse ARP) 9RFC 903) have own MAC, find IP (netbooting is common reason)
- ARP packets nor forwarded, so extension called BOOTP that allowed network booting.
- BOOTP automated by DHCP.

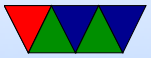


# DHCP

- RFC2131
- To get on network need IP, subnet mask, default router
- Can we automatically get this?
- Dynamic Host Configuration Protocol
- Broadcasts, asking for address
- Server can respond with a fixed one (setup in config file) or handle out dynamically from range
- To avoid need for server on each subnet, can pass through

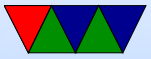


- Broadcast DHCPDISCOVER on UDP port 67.
- All servers send DHCPOFFER on port 68
- Send DHCPREQUEST, respond with DHCPACK
- Timer, needs to re-request before timer is out or server might give to someone else
- DHCP format based on BOOTP



# ICMP

- Internet Control Message Protocol
- Carried as a payload in an IP packet
- Type set to 1
- Codes
  `DESTINATION UNREACHABLE`, Also if MTU is too small but do-not-fragment set
  `SOURCE QUENCH` – should slow transmission rate



(congestion)

`REDIRECT` – try the other router path

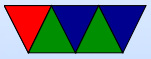
`TIME EXCEEDED` – exceeded TTL, traceroute uses this

`PARAMETER PROBLEM` – illegal value in header

`ECHO`, `ECHO_REPLY` – see if machine is up

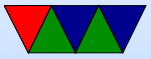
`TIMESTAMP`, `TIMESTAMP_REPLY` – performance debug

- Some sysadmins block ICMP. Why?

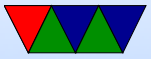


# ping

- Mike Muuss in 1983
  `http://ftp.arl.army.mil/~mike/ping.html`
- Like sonar ping (Hunt for Red October), not any of the backronyms you might find.
- Ping the duck
- ICMP ECHO packet, waits for ECHO reply. Prints timing info, etc.
- Ping of death
- Ping flood

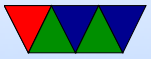


- Broadcast ping to x.x.x.255 (no longer works)
- Used to just say “host is alive”. People would make machines called elvis.



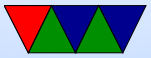
# traceroute

- Van Jacobson in 1987 (also wrote tcpdump)
- Uses ICMP
- *not* tracer-t
- Send packet with TTL=1, when sends ICMP error message know where first hop is
- Send packet with TTL=2, find next
- Linux traceroute sends UDP packets as originally ICMP requests weren't supposed to generate ICMP errors



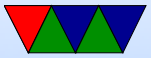
# Linux/UNIX routing setup

- "route" command
- `route add default gateway` sets default gateway (router) for packets leaving the local network
- also set up local subnets you are on, those packets don't need a router
- more complicated if you are configuring your Linux box to *be* a router



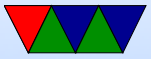
# Out of hosts problem

- IPv4 address exhaustion
- Addresses managed by IANA globally and five regional registrars (RIR)
- Top level ran out in 2011
- 4 of 5 RIRs are out too
- Why are we out?

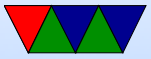


  - Always active connections – unlike dialup, many machine are on all the time
  - So many devices – 4G mobile devices all have one
  - Inefficiencies originally handing out. Companies like Apple, MIT, DEC, all got 16 million address Class A addresses even if didn't need them
  - Despite being out, in 2011 reportedly only 14% of addresses being used

- Why not reclaim unused, such as Class E? The bane of network programmers, the out-of-date router that makes assumptions



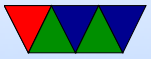
- Stanford gave back a class A in 2000



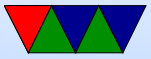
# Network Address Translation

- Private IP ranges, defined in RFC 1919
  10.0.0.0 - 10.255.255.255 (10.0.0.0/8) (one class a)
  172.16.0.0 - 172.31.255.255 (172.16.0.0/12) ( 16 class B)
  192.168.0.0 - 192.168.255.255 (192.168.0.0/16) (256 class C)

- Can use for various reasons, most recently due to network depletion

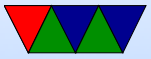


- NAT: map IP addresses from one group to another. often public to private
- NAT and NAPT (port translation) RFC 3022
- Basic NAT has one to one mapping of external to internal IPs
- NATP: based on port, only one external IP
  - Full cone – most common
    once an internal address (iaddr/port) has been mapped to an external (eaddr/port) all packets from iaddr/port



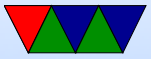
are sent out and any incoming are passed through with no additional checks
  - Restricted cone – same as above, but only external that have received packets from internal can send through
  - Port restricted cone – same as above, but also checks port numbers
  - Symmetric – best security – outgoing packets mapped to different eaddr/port if the destination or port differs

- When passing through, NAT needs to re-write dest/source/port and recompute header checksum



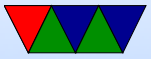
- Linux: IP-masquerade/iptables

- Many IP people hate NAT:
  violates the IP identifies one machine rule,
  hard to connect two machines if both behind different NATs,
  changes IP to be connection oriented, router has to remember connections,
  layering violation, looks at TCP/UDP port numbers,
  only works for TCP/UDP
  Some protocols (like FTP) are even more annoying, send address in plain text in data and that has to be adjusted



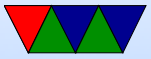
too

can only NAT up to 64k machines



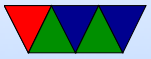
# The Internet Protocol v6

- RFC2460
- Started work in 1991
- Many problems with IPv4. Most notable shortage of addresses.
- IPng. IPv5 was given to an experimental protocol, next is IPv6
- Migration happening, a large amount of web traffic,



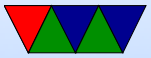
especially that from phones, is already switched.

- *not* backwards compatible
- As of July 2016 12.5% of traffic is IPv6

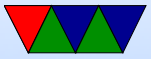


# The Internet Protocol v6 Goals

- Support billions of hosts
- Reduce size of routing tables
- Simplify the protocol (so routers can be faster)
- Better security
- Pay more attention to type of service
- Aid multicasting

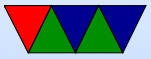


- Allow roaming w/o changing address
- Co-exist with existing protocols

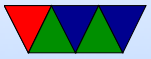


# The Internet Protocol v6 features

- Address size 128 bits
  a lot of addresses. $7x10^{23}$ for ever square meter
- Fixed length header (speeds up processing)
- Quality of service
- Anycast
- autoconfiguration (like DHCP)

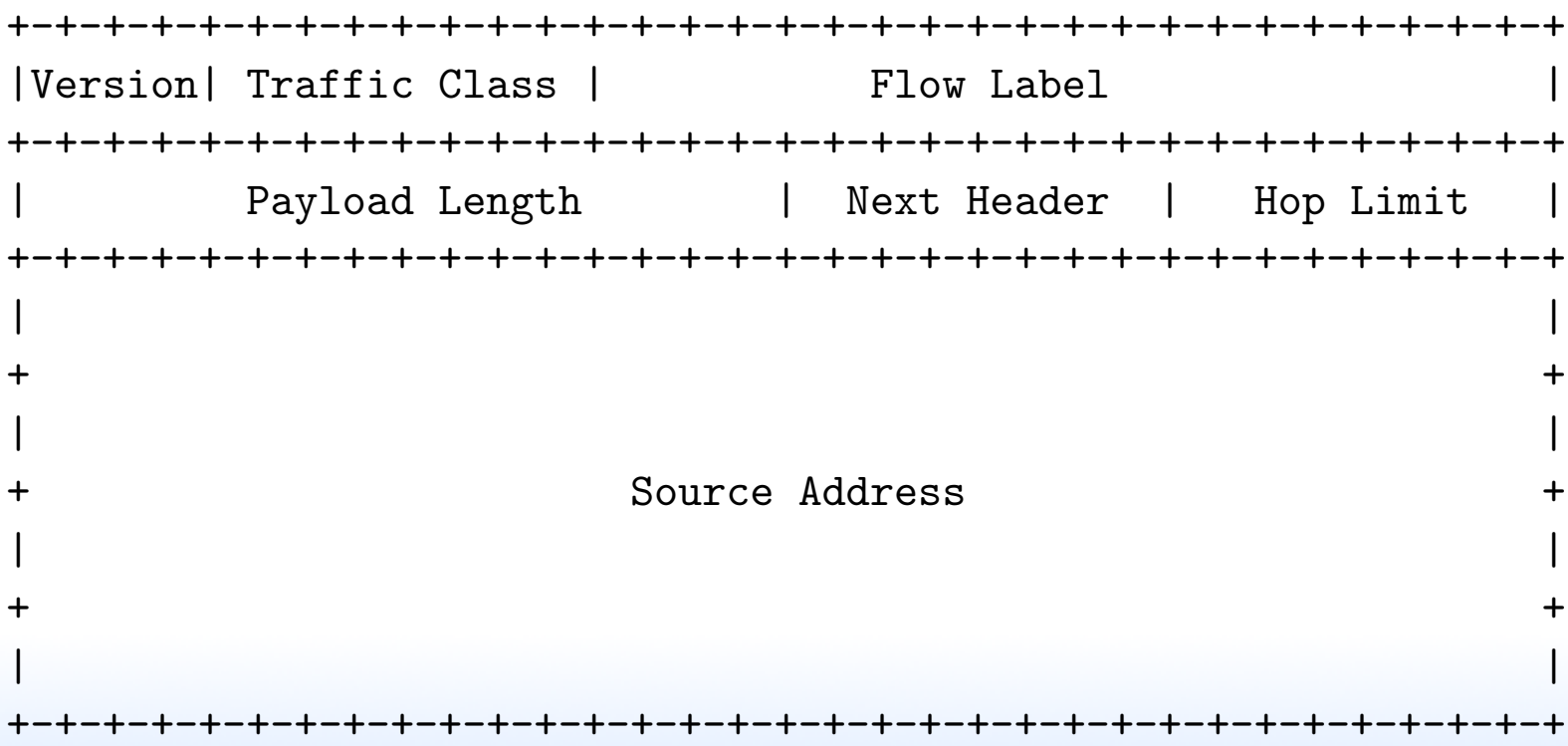


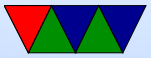
- Fields not really used in IPv4 dropped
- Minimum fragment size 1280 (from 576)
- No checksum – was slow and had to be recalculated often

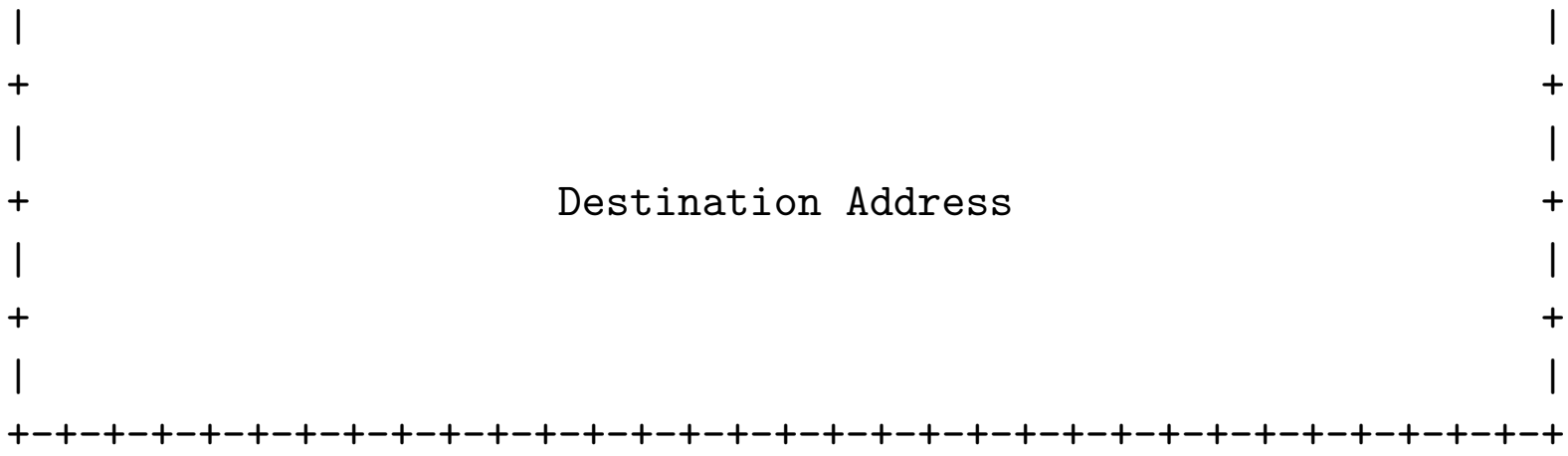


# IPv6 header

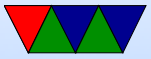
- Header fixed length of 40 bytes, with Extension headers
- ASCII art from RFC 2460



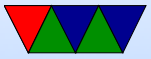






- (1 nybble [4-bits]) Version number = 6
- (8-bits) Traffic class
- (20-bits) Flow label (for streaming?)
- (16-bits) Payload length. 64k (header bytes not counted anymore) (if you want longer, extension for Jumbograms)

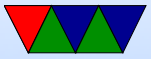


- (8-bits) Next header. If nothing special identifies TCP or UDP If special options (fragmentation, security) indicated
- (8-bits) Hop Limit, TTL, bit debate about whether 8-bits was enough
- (128-bits) Source Address
- (128-bits) Destination Addresses
- Why not 64-bits?

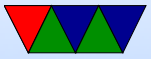


# IPv6 fragmentation

- Fragment header. Routers cannot fragment, only at source
- How can this work when not know MTU?
- Always required to have at least a MTU of 1280 bytes or greater.
- Path MTU discovery protocol to discover MTU along the way (RFC 1981). (IPv4 too, set DNF and get error

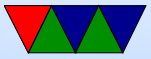


via ICMP) If too big, sends an error back and source needs to fragment it smaller

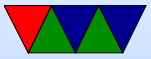


# IPv6 addresses

- Too long for dotted decimal, use colon hexadecimal
- X:X:X:X:X:X:X:X where X is 16 bit chunk
- F000:0123:5678:0000:0000:ABCD:0000:CAFE
- Can drop leading zeros, as well as groups of zeros
  F000:123:5678:::ABCD::CAFE
- Do not have classes RFC 4291

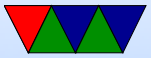


- encoding ipv4 addresses in ipv6?
- autoconfig – generate a unique ID, often based on MAC address and send it to router (Router solicitation). Router sends back router advertisement which has subnet prefix and can be used to generate global address
- ::1 ip6-localhost, fe00::0 ip6-localnet



# IPv6 Extensions

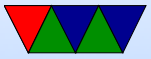
- Security – have MAC in your IPv6 address?



# IPv6/IPv4 compat

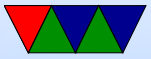
- Dual stack – host runs both IPv4 and IPv6
  or internal is IPv6 but router converts to IPv4 before passing on

- Tunneling – encapsulate IPv6 inside of IPv4, tunnels across IPv4, split back out to IPv6 on other side of tunnel

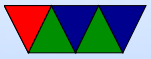


# Internet History

- US Federal government in 1960 robust network
- Packet switch network
- ARPAnet – connected military and academic computers in 1980s
  First in 1969. BBN build equipment, IMP, first router.
  First ARPAnet with 4 IMPS, UCLA, SRI, UCSB, Utah.
  29 October 1969. First message was login (but computer crashed after "lo" and had to be retried)



- 1971 – first e-mail
- 1983 – ftp
- ARPAnet migrate to TCP/IP on January 1, 1983
- NSFnet – 1986 – connect up supercomputing sites
- 1989 – first public commercial connections – before this you were really only supposed to use internet for "official use"
- 1991 – High Performance Computing and



Communication Act of 1991 by Al Gore

- World Wide Web wasn't until 1989/1990
- BSD famously had good free TCP/IP stack, many implementations based on this. Linux is implemented from scratch. Windows (despite rumors due to strings in utilities) is as well.